

**THE UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF MISSOURI**

**IN THE MATTER OF THE  
SEARCH OF:**

**3067 BLUEBIRD ROAD,  
MERRIAM WOODS, TANEY COUNTY,  
MISSOURI 65704**

**Case No. 24-SW-2182-DPR**

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Joseph Neuschwander, a Task Force Officer (“TFO”) with the Homeland Security Investigations, Immigration and Customs Office (“HSI/ICE”), being first duly sworn, hereby depose and state as follows:

1. I am employed as a detective with the West Plains, Missouri, Police Department (“WPPD”) and a TFO with HSI in Springfield, Missouri. I am also assigned to the Southwest Missouri Cyber Crimes Task Force (“SMCCTF”). I have been employed in the field of law enforcement full-time since 2003, including duties as a patrol officer, patrol supervisor, SWAT operator, and detective. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended trainings provided by the Internet Crimes Against Children Program and the Missouri Internet Crimes Against Children (ICAC) Task Force. Additionally, I have attended an approved 35-hour course for Universal Forensic Extraction Device Series (UFED) hardware and software methodology and am a Cellebrite Certified Operator and Cellebrite Certified Physical Analyst.

2. As part of this Affiant’s duties with FBI, I investigate criminal violations relating to child exploitation, and child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

3. The statements in this affidavit are based on my personal observations, training and experience, investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, this

Affiant has not included each and every fact known to me concerning this investigation. This Affiant has set forth the facts necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, are currently located at **3067 Bluebird Road, Merriam Woods, Taney County, Missouri 65704**, a location within the Western District of Missouri.

4. This affidavit is in support of an application for a search warrant for evidence, fruits, and instrumentalities of the foregoing criminal violations, which relate to the knowing possession, receipt, distribution, and/or production of child pornography. The property to be searched is described in the following paragraphs and fully in Attachment A. This Affiant requests the authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

5. This Affiant has probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer, in or affecting interstate commerce, to produce, receive, possess and/or distribute child pornography, are located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

#### **STATUTORY AUTHORITY**

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252, and 2252A, relating to material involving the production, receipt, possession, and/or distribution of child pornography:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of

interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any child pornography, as defined in 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

#### **DEFINITIONS**

7. The following definitions apply to this Affidavit and its Attachments:

a. The term “minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term “sexually explicit conduct,” 18 U.S.C. § 2256(2)(A)(i-v), includes actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term “visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which



is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term “computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to, or operating in conjunction with, such device.

e. The term “child pornography,” as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

i. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

ii. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

iii. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, and paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, and photocopies), mechanical form (including, but not limited to, phonograph records, printing, and typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices

such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

g. “Internet Service Providers” (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

i. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transfer Protocol (HTTP).

## **BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY**

8. Based on this Affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this Affiant has had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

10. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords individuals several different venues for meeting one another, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

13. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Google, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer and/or other electronic devices in most cases.



14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

### **CELLULAR PHONES AND CHILD PORNOGRAPHY**

15. Based on this Affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom this Affiant has had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

16. Cellular phones ("cell phones") are exceptionally widespread. The Central Intelligence Agency estimates that in 2016 there were 416 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images, and the ability to access and browse the Internet.

17. In this Affiant's training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

18. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES**

19. Searches and seizures of evidence from computers and cell phones commonly require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:



a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

20. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media).

21. Furthermore, because there is probable cause to believe that the computer, its storage devices and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

### **BACKGROUND OF INVESTIGATION**

22. On June 24, 2024, the SMCCTF was conducting an online investigation on the BitTorrent network for offenders sharing child sexual abuse material (“CSAM”). An investigation was initiated for a device at an IP address in the Branson, Taney County, Missouri area, because it was associated with a torrent file referencing 428 files, at least one of which was identified as being a file of investigative interest to child pornography investigations. This investigation was assigned to this Affiant.

23. Peer to Peer (P2P) file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet connected devices such as computers, tablets and smartphones running P2P software form a P2P network that allow users on the network to share digital files. BitTorrent is one of many P2P networks. For a user to become part of the BitTorrent network, the user must first obtain BitTorrent software and install it on a device. When the BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users.

24. Users of the BitTorrent network wishing to share new content will use a BitTorrent program to create a “torrent” file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their “infohash”, which uniquely identifies the torrent based on the file(s) associated with the torrent file.

25. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

26. On June 24, 2024, I was conducting an online investigation on the BitTorrent network for offenders sharing CSAM. An investigation was initiated for a device at IP address 47.214.10.210, because it was associated with a torrent with the infohash: 27d196080b19d9c26da853048e0b36c49eac8fd0. This torrent file references 428 files, at least one of which was identified as being a file of investigative interest to CSAM investigations. Using a computer running investigative BitTorrent software, a direct connection was made to the device at IP address 47.214.10.210, hereinafter referred to as "Suspect Device." The Suspect Device reported it was using BitTorrent client software -BL1000- BitLord 1.0.

27. On June 24, 2024, between 1216 hours and 1355 hours, a download was successfully completed of 256 files that the device at IP address 47.214.10.210 was making available. The device at IP Address 47.214.10.210 was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

28. I reviewed the 256 files, and there were files depicting CSAM. For example, one file had the filename "(pthc)sucknew(awesome cumshot).avi" (MD5: 5UDNV6G2MFYSBVJSINYRSG44PVTYTX6W), and was a video file 00:01:36 in length, and depicted a prepubescent female child performing fellatio on an erect male penis, which was the primary focus of the video. The child victim's face was visible in the video, and she appeared to be approximately four to five years of age. Based on my training and experience, I believe this file contained child sexual abuse material (otherwise referred to as child pornography), that is, a visual depiction of a minor engaged in sexually explicit conduct.



29. On June 25, 2024, a query was made on IP address 47.214.10.210 through the American Registry for Internet Numbers (“ARIN”). ARIN reported that IP address 47.214.10.210 was registered to Optimum.

30. On June 26, 2024, I applied for and obtained an investigative subpoena in the Circuit Court of Howell County, Missouri, signed by the Honorable Associate Judge David Ray, directed at CSC Holdings, LLC (DBA Optimum Online High-Speed Internet) to provide subscriber information concerning IP address 47.214.10.210, for June 24, 2024, between 1216 hours and 1355 hours CST. The signed document was submitted by email to CSCHoldingsLLC@netd-ttp.com to the ATTN: Subpoena Compliance c/o Yaana Technologies, LLC.

31. On July 12, 2024, an email response was received from the Yaana Managed Services, identifying the Optimum Online High-Speed Internet subscriber information as Mark RHOADES, **3067 Bluebird Road, Merriam Woods, Missouri 65740**, with the associated email address of “mymomangiel966@gmail.com,” and phone number (417) 559-6006.

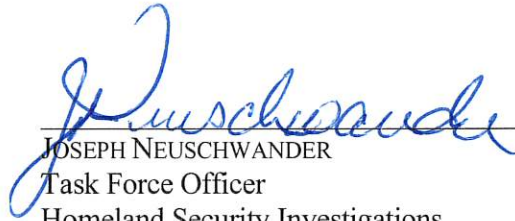
32. Criminal history records obtained from the Missouri Information Analysis Center (“MIAC”) indicates that RHOADES has a length of history with law enforcement including that he is a Caution 1 Violent Offender, has been found guilty of tampering with an utility in the second degree, stealing, assault in the second degree, burglary in the second degree, and assault in the third degree.

33. On July 17, 2024, HSI Special Agent Jeremy Bluto conducted drive-by surveillance at **3067 Bluebird Road**, and provided TFO Neuschwander with images of the property.


#### **PROBABLE CAUSE**

34. Based on the above facts, this Affiant believes probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is

or has been used as the means of committing a criminal offense, namely possible violations of 18 U.S.C. §§ 2251, 2252, and 2252A, including, but not limited to, the items listed in Attachment B. Further Affiant Sayeth Naught.

  
JOSEPH NEUSCHWANDER  
Task Force Officer  
Homeland Security Investigations

Subscribed and sworn to before me via telephone on the 19th day of August 2024.

  
HONORABLE WILLIE J. EPPS, JR.  
Chief United States Magistrate Judge  
Western District of Missouri